GeekBrains

Урок 2 Тема 2

Регистры процессора

Реверс-инжиниринг

В этом видео

1. Память процессора.
2. Обзор регистров процессора x86.
3. Базовые операции с регистрами.
4. Разработка первой программы.

GeekBrains

Семейство процессоров x86

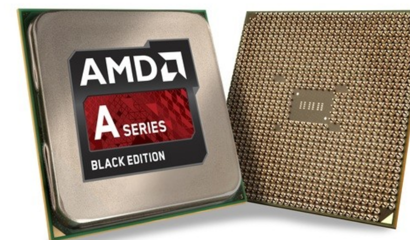
Intel

Архитектура: x86 и x64



AMD

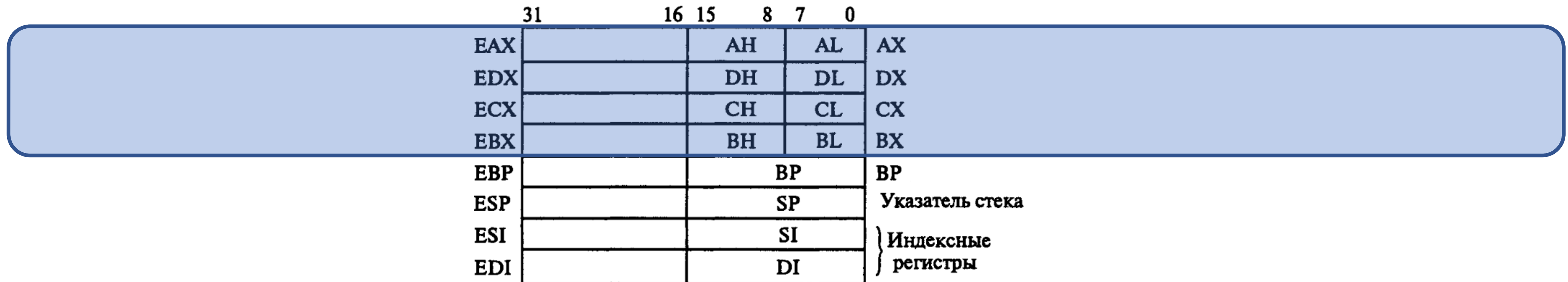
Архитектура: x86 и x64

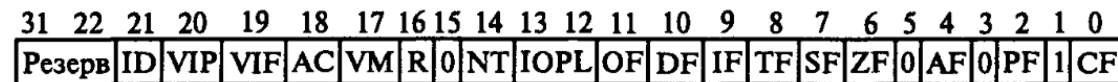


Регистры процессора x86

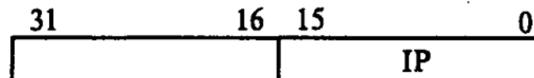
- Регистры общего назначения (EAX, EBX, ECX, EDX).
- Регистры — указатели стека (ESP, EBP).
- Индексные регистры (ESI, EDI).
- Указатель команд (EIP).
- Сегментные регистры (CS, DS, SS, ES, FS, GS).
- Регистр признаков (EFLAGS).

Регистры общего назначения





Регистр признаков EFLAGS



Указатель команд EIP

Регистры — указатели стека

	31 … 16	15 … 8	7 … 0	
EAX		AH	AL	AX
EDX		DH	DL	DX
ECX		CH	CL	CX
EBX		BH	BL	BX
EBP		BP		BP
ESP		SP		Указатель стека
ESI		SI		Индексные регистры
EDI		DI		

31 22	21	20	19	18	17	16	15	14	13 12	11	10	9	8	7	6	5	4	3	2	1	0
Резерв	ID	VIP	VIF	AC	VM	R	0	NT	IOPL	OF	DF	IF	TF	SF	ZF	0	AF	0	PF	1	CF

Регистр признаков EFLAGS

31 … 16	15 … 0
	IP

Указатель команд EIP

GeekBrains

Индексные регистры

	31 … 16	15 … 8	7 … 0	
EAX		AH	AL	AX
EDX		DH	DL	DX
ECX		CH	CL	CX
EBX		BH	BL	BX
EBP		BP		BP
ESP		SP		Указатель стека
ESI		SI		Индексные регистры
EDI		DI		

31 22	21	20	19	18	17	16	15	14	13 12	11	10	9	8	7	6	5	4	3	2	1	0
Резерв	ID	VIP	VIF	AC	VM	R	0	NT	IOPL	OF	DF	IF	TF	SF	ZF	0	AF	0	PF	1	CF

Регистр признаков EFLAGS

31 … 16	15 … 0
	IP

Указатель команд EIP

Регистры состояния и управления

	31–16	15–8	7–0	
EAX		AH	AL	AX
EDX		DH	DL	DX
ECX		CH	CL	CX
EBX		BH	BL	BX
EBP		BP		BP
ESP		SP		Указатель стека
ESI		SI		Индексные регистры
EDI		DI		

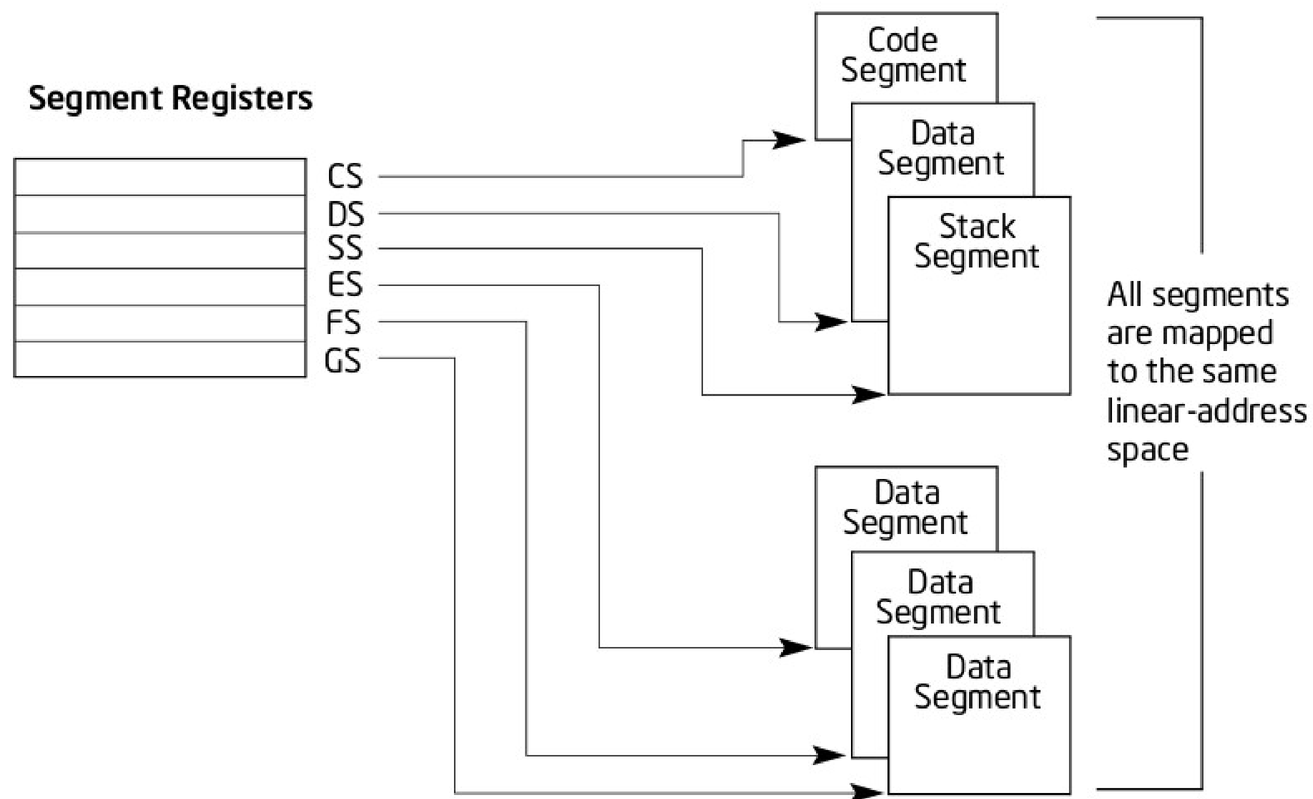
31–22	21	20	19	18	17	16	15	14	13–12	11	10	9	8	7	6	5	4	3	2	1	0
Резерв	ID	VIP	VIF	AC	VM	R	0	NT	IOPL	OF	DF	IF	TF	SF	ZF	0	AF	0	PF	1	CF

Регистр признаков EFLAGS

31–16	15–0
	IP

Указатель команд EIP

Сегментные регистры



Базовые операции с регистрами процессора

mov — переместить (mov eax, 4).

add — сложить (add ebx, 2).

sub — вычесть.

inc — инкремент (inc ecx).

dec — вычесть 1, декремент.

xor — сложение по модулю 2 (xor edx, edx).

```
0x00002b3b      83f301          xor ebx, 1
0x00002b3e      0fb6c3          movzx eax, bl
0x00002b41      488b9c24b800.   mov rbx, qword [var_b8h]
0x00002b49      6448331c2528.   xor rbx, qword fs:[0x28]
0x00002b52      0f8574010000    jne 0x2ccc
0x00002b58      4881c4c80000.   add rsp, 0xc8
0x00002b5f      5b              pop rbx
0x00002b60      5d              pop rbp
0x00002b61      415c            pop r12
0x00002b63      415d            pop r13
0x00002b65      415e            pop r14
0x00002b67      415f            pop r15
0x00002b69      c3              ret
; CODE XREF from main (0x2aa2)
0x00002b6a      4889ea          mov rdx, rbp
0x00002b6d      4c89fe          mov rsi, r15
0x00002b70      bf01000000      mov edi, 1
0x00002b75      e8b6f7ffff      call sym.imp.__lxstat
0x00002b7a      85c0            test eax, eax
0x00002b7c      0f95c0          setne al
0x00002b7f      e939ffffff      jmp 0x2abd
; CODE XREF from main (0x2a95)
0x00002b84      31f6            xor esi, esi
0x00002b86      4889ea          mov rdx, rbp
0x00002b89      bf01000000      mov edi, 1
0x00002b8e      e81dfaffff      call sym.imp.__fxstat
0x00002b93      85c0            test eax, eax
0x00002b95      89c6            mov esi, eax
0x00002b97      0f842bffffff    je 0x2ac8
```

GeekBrains

Итоги

1. Познакомились с регистрами процессора с архитектурой x86.
2. Узнали базовые команды языка Ассемблер для работы с регистрами.
3. Получили опыт разработки программы на языке Ассемблер.

GeekBrains